Two-Factor, Two-Step or Multi-Factor Authentication

Content

- Description
- What is Two Factor, Two-Step or Multi-Factor Authentication
- What is required to use this?
  - Service supporting Two-Factor, Two-Step or Multi-Factor Authentication
    - A smartphone, tablet, RSA token device or Authenticator device
  - Why should we use Two Factor Authentication?
  - How do I set up Two Factor Authentication?
- What are the drawbacks with having this setup?
  - Have to authenticate almost every time you log in.
  - Difficult to recover
  - Certain services require a different way to access for apps
- Related articles

Description

This article is going over what Two-Factor, Two-Step or Multi-Factor Authentication

What is Two Factor, Two-Step or Multi-Factor Authentication

Two-Factor (2FA), Two-Step or Multi-Factor (MFA) Authentication is a security method used by several systems in addition to just the username and password method.

This usually involves another device or list of passcodes that need to be entered after the initial log in.

What is required to use this?

Service supporting Two-Factor, Two-Step or Multi-Factor Authentication

Several services, like Google and Amazon, will offer it as 2-Step Verification or refer to it as adding an Authenticator.

As of December 2020 MFA or a VPN is required for UCPATH and other certain secure websites at UCSB, such as those dealing with financial, job, and personnel matters.

A smartphone, tablet, RSA token device or Authenticator device

Items like an RSA Token device as seen here

<table>
<thead>
<tr>
<th>RSA Token Device (aka RSA FOB)</th>
</tr>
</thead>
</table>

These have been used for some sites but with smartphone apps such as Duo (Website or App Store) or Google Authenticator (Google Play or App Store), you can make your smartphone or a tablet device act as an Authenticator device for such sites.
Why should we use Two Factor Authentication?

The point of the Two Factor Authentication is to help verify that you are the person accessing the site in question. Often times, passwords get compromised, however, an Authenticator is a special key that only you should have on hand. Apps like Duo, Google Authenticator or the RSA Token Device will have a random number generated for a short period of time that it is validated by the server. So while someone can steal your password, the second step will make it a little difficult for someone to access your account if they don't have your authenticator. This is also handy for situations such as accessing something sensitive on a computer that is in public, as it is easy to capture passwords on a shared computer that is compromised, but with an authenticator, it makes it much harder to exploit that.

How do I set up Two Factor Authentication?

It will depend on the service you are with. For the most part, just log onto the service you want to enable and follow the instructions. UCSB uses Duo for UCPath and several other services and has instructions posted per service as well as general instructions:
https://www.it.ucsb.edu/mfa/getting-started-mfa-duo
https://www.it.ucsb.edu/mfa/adding-multiple-devices-mfa-duo

What are the drawbacks with having this setup?

Have to authenticate almost every time you log in.

In most cases, especially if you are connecting with a device or computer that you don’t own, you will have to prove who you are every time. Which means you will need to have the authenticator available almost all the time.

Difficult to recover

If your authenticator gets misplaced, damaged or stolen (ie. your phone or tablet), you may need to go through some extra hassle and time to get things cleared up with the service to help you re-establish your account access.
https://www.it.ucsb.edu/mfa/enroll-replacement-cell-phone-duo

Certain services require a different way to access for apps

In the case of GMail, where some people like to use Thunderbird or some other Mail Client program, which only knows how to handle Username and Password, this can cause problems with access as they don’t support a means to make use of the Two Factor Authentication. You may have to refer to that service's alternative password means, such as Google's App Password service, which generates a unique password to be used for a particular application. (Reference: https://support.google.com/accounts/answer/185833?hl=en)

This also happens if you use a Personal GMail account trying to access your UCSB Connect EMail for sending purposes.

Related articles

- Two-Factor, Two-Step or Multi-Factor Authentication
- Securing a computer on Campus
- UFW - Basics
- Digital Piracy
- Securing Linux Computer